

LegacyTexas Bank

LegacyTexas Bank is a full-service community bank serving businesses and families throughout North Texas with 19 branches, 350 employees and over \$1.6 billion in assets. Network and information security is absolutely vital, as is compliance with FFIEC and FDIC regulations.

With nearly 50 years under its belt, LegacyTexas Bank has earned the trust of tens of thousands of individuals and businesses in the Lone Star State by staying a step ahead of the industry. It was one of the first to introduce ATMs in Texas and was first in the region to bring branch-banking locations to customers.

Log and Event Management Challenge

Now, in the face of thousands of data breaches a year putting massive amounts of personal and business information at risk, LegacyTexas Bank is focused on keeping customer trust with a state-of-the-art security profile.

Even with three members of its IT department spending 50+ hours a month manually reviewing logs, staying ahead of potential information security threats was a challenge for LegacyTexas Bank.

“Manually inspecting more than a quarter of a million lines of log code every month across all of our devices just wasn’t possible,” said Jon Drake, CIO, LegacyTexas Bank. “Our team was only covering a small portion of our logs monthly, leaving far too much at risk.”

In addition to LegacyTexas Bank’s own security concerns, bank examiners are becoming increasingly stringent about how banks handle log data. FFIEC regulations require banks to aggregate all device logs and store them in a secure location. Now, regulators are also asking banks to keep logs for two years or more for forensic purposes.

“That’s a lot for a bank to tackle — and virtually impossible without an automated approach,” said Drake.

LegacyTexas Bank needed technology that could automate log management and take action in real-time when potential threats or violations were discovered — keeping compliance requirements front-of-mind including log aggregation, analysis, reporting, storage and rapid retrieval.

Solution

LegacyTexas Bank’s IT team saw a 15-minute demo of SolarWinds Log & Event Manager (LEM) at a midsize enterprise event and was instantly convinced that it was exactly what the bank needed to address its security and compliance challenges.

SolarWinds LEM was the only network security solution that offered LegacyTexas Bank’s IT team the visibility into network activity it needed to meet industry compliance requirements and effectively monitor and protect the network.

SolarWinds LEM’s ability to provide instant insight and context for events helps to uncover potential threats and stops unauthorized installation or use of third-party applications. SolarWinds LEM’s compliance-ready reports exceed requirements for regulations such as FFIEC and FDIC — giving LegacyTexas Bank the upper hand with auditors.

“In the interest of due diligence we looked at quite a few other security information and event management solutions, but none of them can take action when suspicious or unauthorized activity is detected,” said Drake. “Other solutions on the market can’t even do half of what SolarWinds LEM does.”

SolarWinds LEM was up-and-running less than 45 days after LegacyTexas Bank’s team discovered it — monitoring and reporting on a network of more than 225 nodes, including switches, routers and firewalls.

CLIENT STATISTICS

\$1.6 billion in assets

19 branch locations

350 employees

“We could hire five skilled staffers at 40 hours a week just to comb through logs — a reactive approach riddled with human error — and we still wouldn’t come close to the coverage we get with SolarWinds LEM,” said Drake.

Results

LegacyTexas Bank uses SolarWinds LEM to protect its entire network — with a strong focus on Active Directory.

“Just two days after installing SolarWinds’ solution, I noticed a local admin trying to log onto the network, but I couldn’t figure out where it was coming from,” said Drake. “I logged onto SolarWinds LEM and found all of the information that I needed in less than ten seconds.”

LegacyTexas Bank chose SolarWinds LEM for its:

- **Complete visibility and instant alerts** on what’s happening on the network, allowing LegacyTexas Bank’s IT team to see exactly who’s logging on, and at what authority level — with full ability to quarantine, block, route and control services, processes, accounts and privileges.
- **Real-time correlation and analysis of network activity** — providing instant insight and context for each event while uncovering potential threats.
- **More than 700 pre-configured correlation rules** and dozens of active responses that help LegacyTexas Bank quickly address security and compliance concerns — such as adding new users to Active Directory, managing account lockouts or stopping unauthorized installation or use of third-party applications.
- **Compliance-ready reports** that exceed requirements for regulations such as FFIEC and FDIC — and blow the auditors away.

In an effort to stay ahead of network threats, LegacyTexas Bank hires outside auditors to regularly conduct internal penetration tests and identify vulnerabilities.



SolarWinds LEM quickly identifies attacks, highlights threats, and uncovers policy violations with real-time log analysis and powerful event correlation.

“After a week-long test of our network security, we sat down with the firm and told them exactly what they attempted to do on our network before they could say a word. The shocking look on their faces spoke volumes about the power of SolarWinds’ solution.”

We could hire five skilled staffers at 40 hours a week just to comb through logs — a reactive approach riddled with human error — and we still wouldn’t come close to the coverage we get with SolarWinds LEM,” said Drake.

IT Management Inspired by You.

SolarWinds (NYSE: SWI) provides powerful and affordable IT management software worldwide — from Fortune 500 enterprises to small businesses. We work to put our users first and remove the obstacles that have become “status quo” in traditional enterprise software. SolarWinds products are downloadable, easy to use and maintain, and provide the power, scale, and flexibility needed to address users’ management priorities. Our online user community, thwack, is a gathering-place where tens of thousands of IT pros solve problems, share technology, and participate in product development for all of SolarWinds’ products.

solarwinds.com

solarwinds 

3711 S. MoPac Expressway, Building Two, Austin, TX 78746
T: 866.530.8100 | F: 512.682.9301

©2010 SolarWinds, Inc. All rights reserved. SolarWinds®, the SolarWinds logo, ipMonitor®, LANsurveyor®, and Orion® are among the trademarks or registered trademarks of the company in the United States and/or other countries. All other trademarks are property of their respective owners.